Thirteen³

# Investigation Request:

# Chaos at Cobalt

## A cross-platform investigation

Cobalt Edge Technologies seeks your help investigating a compromise affecting both Windows and Linux systems.

**Can you crack the case?**

# Investigation Request:
# Chaos at Cobalt

Cobalt Edge Technologies recently expanded its IT footprint, launching a new email system and website.

Employees responded positively, but inexperienced staff failed to keep several applications updated.

Shortly after the website went live, a threat actor gained access and began moving laterally within the network.

Some unusual activity was noticed, but a full domain compromise occurred before containment began.

# Investigation Request:
# Chaos at Cobalt

The evidence collected includes both disk and memory images from four systems within the Cobalt Edge network:

### CHI-L-WEB-04

Ubuntu 24.04 LTS
web server
running WordPress

### CHI-L-CONF-01

AlmaLinux OS 10
server hosting Confluence

### DESKTOP-9RQ7DGC

Windows 11 25H2
user workstation

### CHI-W-ADDC-01

Windows Server 2025
domain controller and mail server (cobaltedge.xo)

## Your Goals

Identify the threat actor's path through the environment

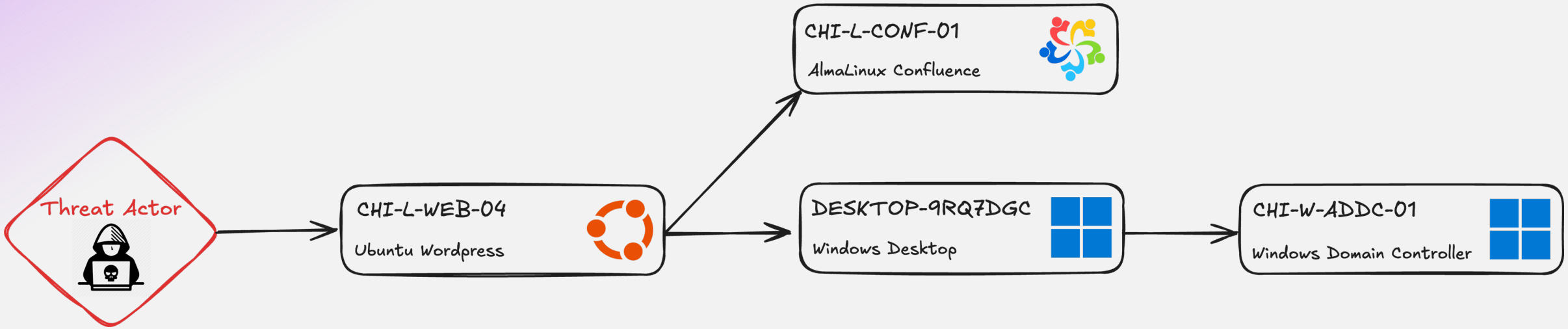
Determine what data was exfiltrated

Locate any persistence mechanisms left behind

# STOP HERE!

The next section will take you through what the threat actor did, so hold your horses until you complete your analysis!

# Lateral Movement Overview




Visualization of lateral movement and relationships between all four systems within the environment.

# So, What Actually Happened?

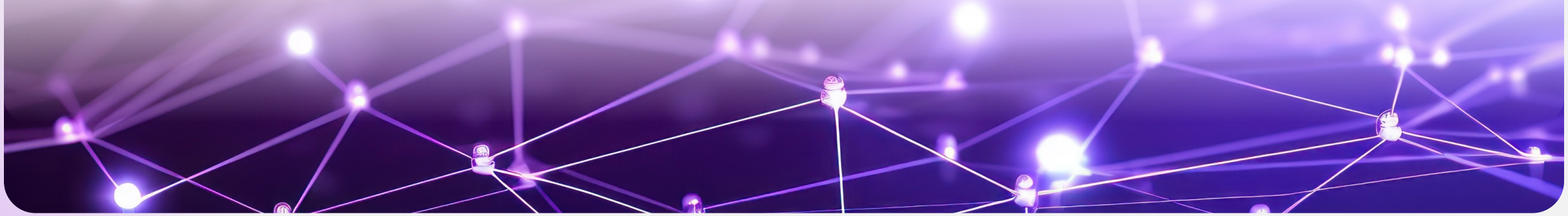
## Initial Access and Foothold on CHI-L-WEB-04

Initial access occurred via an outdated plugin on the company's WordPress site.

- Once the foothold was established, the threat actor exfiltrated Firefox profile data, Bash history, and /etc/shadow.

Credentials recovered from this host were used to gain SSH access with elevated privileges and exfiltrate the WordPress database.

- Persistence was achieved by modifying a MySQL startup script and configuring Cloudflare tunnels for remote access.



# So, What Actually Happened?

## Lateral Movement Across CHI-L-CONF-01 and DESKTOP-9RQ7DGC

From the web server, the threat actor pivoted to **CHI-L-CONF-01**, exploiting a Confluence vulnerability for reconnaissance.

- Using credentials from **CHI-L-WEB-04**, they obtained full access and exfiltrated Firefox profile data and the PostgreSQL database.

Leveraging stolen credentials, the threat actor pivoted to **DESKTOP-9RQ7DGC**, read email data, disabled security tools, and exfiltrated documents.

- A new local account was created for future access.

A domain administrator noticed suspicious activity and began investigating.

# So, What Actually Happened?

## Domain Compromise on CHI-W-ADDC-01

Captured RDP credentials from the administrator's session enabled lateral movement to **CHI-W-ADDC-01** (domain controller and mail server).

- The NTDS.dit Active Directory database and mail server contents were exfiltrated.

With a full domain compromise achieved, the threat actor began exfiltration of all collected data.

The administrator recognized the intrusion and initiated incident response procedures to preserve evidence.